--------- (END CUT AND PASTE SECTION - USPTO PPA & DDP)----------

---

REMARKS SECTION (Amendment A response to the patent examiner's 1st Office Action Dated: 09/12/2007):

A.B. declares as follows:

1). I am the applicant in the above application.

2). In response to the USPTO Office of Patent Examiner's, 1st Office Action dated 09/12/2007 and mailed to the present applicant, this USPTO Amendment A response is submitted.

Present applicant responds as follows.

General Remarks:

The present applicant proposes the following changes in the patent specification's new material section, in order to generally comply with the patent examiner's 1st office action objections, while also under the MPEP rule 118, adding of 0% of 'new technical material,' merely wishing to restore excerpted, 'original material' of the present applicant's USPTO's DDP and USPTO's PPA programs on archived file storage with the USPTO, which was truncated by the USPTO's

Office of Initial Patent Examiner's (OIPE) to gain temporary brevity, prior to the USPTO's original patent application archiving.

To clearly distinguish over the prior art of Narin et al, (DiFonzo is assumed as post-art to the present applicant's invention), the new technical material as legally claimed in the claims section (35 USC Section 112), the present applicant proposes to emphasize the 'prior art' and thus present applicant non-claimed, lower level crpyto-hardware component, of the present applicant claimed cryptographic systems architecture, which in the present applicant's current and past process patent claims is referenced as a 'provided by' assumed pre-existing, hardware component (e.g. prior art, US Federal National Institute of Standard's (NIST's) Clipper chip/Capstone program. e.g. crypto-digital signal processor (C-DSP) unit 932), which also will be claims narrowed to emphasize an additional prior art, lower level systems component, 'provided by' crypto-operating system (C-OS) component (e.g. US Federal NIST's Clipper chip/Capstone program operating system, e.g. Various MIL-STD 'red/black' Operating Systems).

SPECIFICATION SECTION: The present applicant wishes to comply with the USPTO's MPEP Rule 118, adding of 0% new technical material rule, while also restoring key excerpts, of the present applicant's USPTO Document Disclosure Program (DDP) and USPTO Provisional Patent Application (PPA's), brief and original 'BACKGROUND section,' officially removed by the USPTO's Office of Initial Patent Examiner's (OIPE), from the original patent application (patent application No.:

10/755,624, filing date: 06/06/2004) in order to produce brevity, but, present applicant contained as 'original technical material' in both the present applicant's:

Provisional Patent Application (PPA Number: 60/441,189, Dated: 1/21/2003), and also including the present applicant's:

Document Disclosure Program (DDP Serial Number: 510,730, Dated: 5/1/2002).

The present applicant wishes in a similar manner, to restore key excerpts of the 'original technical material,' which was OIPE removed to produce brevity, in the patent application no.: 10/755,624, filing date: 06/06/2004, being only key portions of 'new technical material,' including the brief crypto-hardware background discussion in the present applicant's PPA document.

The present applicant in a similar manner, proposes changes to the present applicant's CIP patent specification section's, new technical material description of the present patent, present applicant wishes to propose restoring only key excerpts of USPTO DDP document's 100% already submitted, and officially USPTO document archived, and USPTO time and date stamped, 'original technical material,' including the highly relevant, USPTO Office of Initial Patent Examiner's (OIPE) truncated, PARTS NUMBERS Section, as removed by the Office of Initial Patent Examiners (OIPE) for producing brevity, but, contained as 'original technical material' of both the present applicant's:

Provisional Patent Application (PPA Number: 60/441,189, Dated: 1/21/2003), and/or the present applicant's: Document Disclosure Program (DDP Serial Number: 510,730, Dated: 5/1/2002).

In a similar manner the present applicant wishes to restore only the key excerpts of the 'original technical material' which was OIPE removed to produce brevity, in the patent application no.: 10/755,624, filing date: 06/06/2004, being the brief crypto-hardware new art, components discussion in the present applicant's PPA document.

The present applicant proposes to the patent examiner, in addressing the patent examiner's REMARKS regarding overly wordy claims becoming un-workable, that the present applicant convert by simply removing some of the overt claims legal language, to convert some of the more wordy original, regular patent application claims, into a current invention's supplemental technical material section on 'crypto-hardware, being a lower level hardware component ("providing of" process patent claim background hardware component) of this present patent, along with crypto-operating systems (C-OS's) ("providing of" process patent claim background software component) of the somewhat higher logic level of this current patent application, used with the above crypto-hardware background material.

In a similar manner, present applicant wishes to restore 'original technical material' of the OIPE removed from the original patent

application to produce brevity, 'Pressman paragraph,' which was in the original PPA document, and the DDP document.

REMARKS SECTION: Present applicant's proposed AMENDMENT A proposed changes to the 1st regular patent application's (RPA) claims and their proposed implementation, pending patent examiner approval, are covered in detail in this REMARKS Section (with black ink signature, and signature dating, plus USPS Xpress mail No. and USPS Postal Office of Mailing).

CLAIMS SECTION: Current RPA claims section with USPTO status NOTATIONS.

DRAWINGS SECTION: Present applicant's USPTO Drawing Revision Request Form (deferred until patent examiner drawing changes approval).

Present applicant's 'red-inked' requested changes to the RPA drawings, are covered in the REMARKS Section (1st Office Action dated: 09/12/2007), with the actual proposed, 'red-ink' drawing changes presented here.

DETAILED REMARKS (TO 1ST OFFICE ACTION DATED: 09/12/2007):

SPECIFICATION SECTION:

The present applicant wishes to add a small clarifying NOTE to USPTO's Publication No. US 2005/0195975 A1, Dated: 09/08/2005, page 4, paragraph 85, which is not an obvious correction as underline indicated.

The present applicant wishes to correct a small obvious mistake on page 5, paragraph 121 as strike-through indicated (as made obvious by the added NOTE just above).

The present applicant wishes to correct a small obvious mistake on the USPTO published patent application, page 16, paragraph 314, as strike-through indicated, where a PrK-B was used to public key encrypt the value crossed out in strike-out text, instead of an obvious PuK-B which was substituted in corrected add-in under-lined text.

P.A. OBJECTION 1: Patent examiner's objection to the patent examiner chosen, abstract drawing FIG. 7, being patent examiner noted as having commercial trademarks, allowed under the latest USPTO MPEP rules only for unavoidable situations, meant to avoid commercialization of USPTO procedures, also with a non-allowed FIG. number in the abstract text,

since, the MPEP rules specify that the patent examiner will select the best overall representative, abstract drawing.

PRESENT APPLICANT PROPOSES REMOVAL OF THE FIG. 7 WORDS FROM THE PATENT ABSTRACT. PRESENT APPLICANT PROPOSES FOR PATENT EXAMINER APPROVAL, ENCLOSED IN THE DRAWINGS SECTION OF THIS AMENDMENT A RESPONSE, THE OFFICIAL USPTO DRAWING REVISION REQUEST FORM OMITTED UNTIL PATENT EXAMINER APPROVES PRELIMINARY DRAWING CHANGES, DONE BY 'FREE-HAND' WITH RED-INK MARKINGS UPON THE ORIGINAL DRAWING FIG. 7, ARE THE 'RED-INK' HAND DRAWN IN PRELIMINARY DRAWING CHANGES: The present applicant respectfully requests the patent examiner to allow the submission by the present applicant, included in the 'red-ink' and hand drawn rough drafts of removal of all commercial trademarks, also paired with proposed CAD, final drawings FIG 7.

P.A. OBJECTION 2: The patent examiner's objects to the present applicant introducing commercial trademarks and paragraphs structure in the claims.

THE PRESENT APPLICANT PROPOSES REMOVAL OF THE COMMERCIAL TRADEMARKS AND THE PARAGRAPH INDENTATIONS AND 'VERBOSE NATURE' OF THE CLAIMS (THE USPTO OFFICE OF INITIAL PATENT EXAMINERS (USPTO OIPE) HAD FOUND THE ORIGINAL SUBMITTED ON 05/05/2004 AND USPTO OIPE REJECTED CLAIMS, 'NOT DEFINING OVER PRIOR ART OR LACK OF NOVELTY (35 USC SECTION 102), AND HAD REQUIRED INITIAL SUBMISSION, CLAIMS NARROWING FOR THE USPTO'S OIPE, AT LEAST 1 PATENTABLE CLAIM REQUIREMENT, COMPLIED WITH BY THE PRESENT APPLICANT WITH ADDED DETAILS, RATHER THAN MORE ACCEPTABLE, CLAIMS

LANGUAGE PREFERABLE, DEPENDENT PROCESS CLAIMS ADDED DEPENDENCY STEPS, IN RETROSPECT, PRESENT APPLICANT DONE IN SOMEWHAT OVER-VERBOSITY).

P.A. OBJECTION 3: The patent examiner objects to the "indefinite" nature of claim 29, "for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention."

THE PRESENT APPLICANT STATES THAT THE MORE DETAILED AND NARROWED CLAIMS, WORDING WAS ADDED ONLY AFTER USPTO OFFICE OF INITIAL PATENT EXAMINER'S (USPTO OIPE) REJECTIONS OF THE ORIGINAL PATENT APPLICATION'S CLAIMS, DUE TO 'NOT DISTINGUISHING CLEARLY OVER THE PRIOR ART THE NATURE OF THE INVENTION OR LACK OF NOVELTY [35 USC SECTION 102],' AND THAT THE PRESENT APPLICANT PROPOSES THAT THE 'NEW CLAIMS' SHOULD BE MADE LESS VERBOSE, AND MORE CONCRETE WHILE NOT INCLUDING ANY PRIOR ART, BY INCLUDING MORE DEPENDENT CLAIMS, ALSO FOCUSING HIS OWN PRESENT INVENTION, UPON A RELATIVELY MORE HIGHLY SECURE, ASSUMED REQUIRED, CRYPTOGRAPHIC HARDWARE ARCHICTECTURE, USING REQUIRED 'CRYPTO-MEMORY TO CRYPTO-MEMORY' TRANSFERS OF CRYPTOGRAPHIC DATA. THE USPTO HAS RECOGNIZED IN PAST VERY COMPLEX, HARDWARE ARCHITECTURE SYSTEMS PROCESS PATENTS, THAT THE TECHNICAL MATERIAL AND COMPLEX PROCESS CLAIMS RUN UPON THE RELATIVELY LONGER IN PAGES, SIDE (ALTHOUGH TYPICALLY NOT AS LONG AS A DNA OR PROTEIN SEQUENCING CHEMICAL DNA SEQUENCING PROCESS PATENT).

P.A. OBJECTION 4: The patent examiner objects to the "claim directed to non-statutory subject matter", nature of claim 37 as a violation of

35 USC 101. "Applicant is seeking to claim source code, which is considered an abstract idea."

THE PRESENT APPLICANT PROPOSES A MORE LEGAL USE OF THE USPTO ALLOWED, SYSTEMS PROCESS PATENT CLAIMS FOR A COMBINED HARDWARE AND SOFTWARE COMPUTER SYSTEMS INVENTION, BY MAKING MORE LIBERAL USE OF "USING SAID [PROVIDED BY HARDWARE COMPONENT OR SOFTWARE COMPONENT N]" CLAIMS STRUCTURE, MORE CLEARLY IDENTIFYING THE SOFTWARE/FIRMWARE PROCESSING STRONG CRYPTOGRAPHY STEPS, AND WRITING OF THE RESULTS BACK TO COMPONENT N,

P.A. OBJECTION 5: The patent examiner objects to the "similar problems as those listed above [for claims 29 & 37]" nature of claims 29 - 65. Thus "the examiner interprets the claimed invention in view of the Abstract as provided by the applicant."

THE PRESENT APPLICANT STATES THAT THE MORE DETAILED AND NARROWED CLAIMS, WORDING WAS ADDED ONLY AFTER USPTO OFFICE OF INITIAL PATENT EXAMINER'S (USPTO OIPE) INITIAL REJECTIONS OF THE ORIGINAL PATENT APPLICATION'S CLAIMS, DUE TO 'NOT DISTINGUISHING CLEARLY OVER THE PRIOR ART THE NATURE OF THE INVENTION OR LACK OF NOVELTY [35 USC SECTION 102],' AND THAT THE PRESENT APPLICANT PROPOSES THAT THE 'NEW CLAIMS' SHOULD BE MADE LESS VERBOSE, AND MORE CONCRETE WHILE NOT INCLUDING ANY PRIOR ART, BY INCLUDING MORE DEPENDENT CLAIMS.

THE PRESENT APPLICANT PROPOSES A MORE LEGAL USE OF THE USPTO ALLOWED, SYSTEMS PROCESS CLAIMS FOR A COMBINED HARDWARE AND SOFTWARE COMPUTER

SYSTEMS INVENTION, BY MAKING MORE LIBERAL USE OF "USING SAID [PROVIDED BY HARDWARE COMPONENT OR SOFTWARE COMPONENT N]" CLAIMS STRUCTURE, MORE CLEARLY IDENTIFYING THE SOFTWARE/FIRMWARE PROCESSING STRONG CRYPTOGRAPHY STEPS, AND WRITING OF THE RESULTS BACK TO COMPONENT N.

P.A. OBJECTION 6: The patent examiner objects to the obviousness [35 USC Section 103(a)] for claims 29 - 65, due to the prior art of Narin (USPTO Issued Patent No.: 7,185,363).

The present applicant thanks the patent examiner for discovering the highly relevant prior art of:

CASE 1: Attila Narin et al (US Issued Patent Pub. No.: 7,185,363 B1, Issue Date: 02/27/2007, USPTO Application No.: 10/265,437, USPTO App. Filing Date: 10/04/2002), and

discovered through the patent examiner's diligent, official USPTO patent search, which was missed in the present applicant's own personal patent search on the USPTO Web sight, and also the present applicant's Delphion (R) commercial patent database Web sight.

NARIN ET AL PATENT BRIEF SUMMARY AND BRIEF AND HIGHLY RELEVANT PARTS LISTING: The present applicant states that the Narin et al patent, was specifically designed for a technical environment to do 'trusted, proxy server' private key digital signatures, the most frequent case being a privately owned, lap-top computer (e.g. airport for profit, commercial kiosk, or else a public commercial, coffee shop 'hot-spot'), wireless network inter-linked with a 'trusted' commercial, 3rd party owned, kiosk, the latter allowed to do global Internet/Web private key, digital signatures as 'trusted proxy' for the former (e.g. credit card purchases, airline ticket purchase, on-line digital signatures). This similar W. European, publicly placed, 3rd party for profit, kiosk idea

has been widely used prior to wireless private laptops, using W. European smart cards inserted directly into public, 3rd party owned, commercial kiosk systems for many years, including using prevalent public key cryptography private key digital signatures. The W. European contact edge for the 1980's, and contact IC face for the 1990's, and smart cards were based upon crypto-micro-controller technology. The RADIO frequency ID (RFID) or wireless and battery-less (using input RF input output signal piggy-backing (transducing) of only very low digital bandwidth unique serial ID numbers), smart card was a MIT invention during the early 1990's, of adding a very low-cost, wireless Bluetooth RF transceiver IC to a pre-existing smart card. An obvious upgrade function existed for prevalent W. European smart card based kiosk systems (the very poor 99% up-time (2 sigma reliability) W. European phone lines basically forced W. European stand-alone and more expensive, smart card use, vs. the 99.999% up-time (6 sigma reliability) of AT&T (R) quality US phone lines allowing ubiquitous use of very low cost, magnetic strip cards).

An intervening 1990's technology, was use of wireless laptop computers with public kiosks (e.g. airport kiosks, coffee shop wireless 'hot-spots'), importantly without any smart card based public key technology, and also wide open to open air wiretapping fraud which was quite easy using IEEE 802.3 b/c/g radio frequency (RF) scanners.

The early 2000's, new art or invention in the Narin et al patent, was then introducing the wireless lap-top, importantly with only a very brief, 'teach, show, or instruct,' 2 line of Narin issued patent text

reference [Narin, column 9, lines 50 - 54] to a suggested only, optional smart card with a unique customer ID number, used to eliminate the password authentication process, working in 'custom cipher-text' wireless conjunction with a new generation of public kiosks based upon standard early 1990's era, PC technology, while the Narin et al, public key cryptography was standard application of add-on software, using instead standard PC hard disk drive (HDD) 141, ROM 131, and RAM 132. The entire Narin et al kiosk PC, just like a bank ATM PC, applying to prior art to Narin et al, standard public key cryptography processes, must be kept under lock and key and video camera security, and also be kiosk PC custodial security protected from hackers breaching the kiosk system, as a single physical, 'trusted computing unit,' otherwise hackers can easily breach the system and wiretap off crypto-keys, or plant a favored hacker tool of 'keyboard capture buffers,' used to steal crypto-keys.

The Narin et al's server 306, is the Digital Rights Management (DRM) server, the device 304 (e.g. Active-X control or browser plug-in) is wireless laptop resident software, the Narin tethered device 302 (e.g. Web browser software for a hand-held computer), is the software doing graphical user interface (GUI) processing, the kiosk device 200, has a pre-embedded, public key pair. Narin very briefly in 2 lines (column 9 lines 50 - 54), proposes a suggested only, 'smart chip' with custom customer ID be optionally used to replace the FIG. 7 authentication screen of entering an "ID:____", and "Password:____".

NARIN ET AL PATENT'S PROBLEM 1: Importantly Narin et al lacks any fairly permanent, plug-in card crypto-memory (e.g. industry standard Dec. y. 2003, clearly post-art to the present applicant's original USPTO DDP and USPTO PPA material, introduced non-profit, Trusted Computing Group (R) (TCG (R) (www.trustedcomputinggroup.org))) for Narin et al's kiosk server, instead Narin et al uses only early to mid-1990's era standard PC technology. Narin does not allow key 'crypto memory to crypto memory' or crypto-vault analogy, transfer of strong cryptography crypto-keys, being composed of: secret keys from secret key cryptography, 1-time use only secret keys called session keys, group use secret keys called family keys, or private keys from public key cryptography (and even often used public keys for convenience, but, not for privacy).

NARIN ET AL PATENT'S PROBLEM 2: Narin et al also lacks any type of even more advanced in y. 2007, crypto-micro-processor with built-in crypto-memory and 'crypto-core' features (e.g. US National Institute of Standards and Technologies (NIST's) Clipper chip (a strongly suspected ASIC chip implementing the classified, Skipjack secret key algorithm)/Capstone program of the y. 1993 [(standard software engineering public key cryptography textbook reference) B. Schneier, Applied Cryptography, pp's 328, 591 - 593]. e.g. Non-profit Trusted Computing Group (www.trustedcomputinggroup.org) of Dec. y. 2003, clearly post-art to the present applicant's original USPTO DDP and USPTO PPA material), specifically designed with built-in Tamper Resistant Non-Volatile Electrically Erasable Programmable Read Only Memory (TNV-EEPROM) to keep crypto-keys safe from hackers doing

sophisticated wiretapping and pin prober attacks. A hacker getting physical access to a Narin kiosk's PC, through breaching of lock and key, commercial security levels 'trusted platform' security of the kiosk, can easily wiretap off crypto-keys, and can plant hacker favored hacking tools (e.g. keyboard capture buffers, Trojan Horses, viruses, malware, cookies, etc.) used to easily obtain passwords, PIN numbers, credit card numbers, and more importantly: secret keys, private keys, and any family keys and session keys. The Narin et al, device 304 (e.g. wireless laptop computer) and also the Narin et al's, tethered device 302 (e.g. a hand-held computer), are both also highly hacker vulnerable with standard hacker tools of the trade: keyboard capture buffers used to easily gain passwords/passphrases/passcodes, Trojan Horses, viruses, malware, cookies, etc..

THE PRESENT APPLICANT'S PRESENT PATENT APPLICATION IS DEFINITIVE OVER THE OLDER, HIGHLY HACKER VULNERABLE, PRIOR ART OF NARIN ET AL, BY DEFINING OF HIGHLY HACKER RESISTANT, 'NEW ART' ("PROVIDING OF" PRESENT APPLICANT PROCESS PATENT CLAIMS DESCRIPTIONS) OF 100% CRYPTOGRAPHIC LOWER-LEVEL, HARDWARE COMPONENTS (C-DSP, C-uP, C-PC, C-HW), COMBINED WITH LOWER LEVEL SOFTWARE OF CRYPTO OPERATING SYSTEMS COMPONENTS (C-OS), INTEGRATED INTO THE PRESENT APPLICANT'S HIGHER LEVEL CRYPTOGRAPHIC SYSTEMS ARCHITECTURE: 1STLY, DIVIDING THE LOWER LEVEL PC HARDWARE AT THE COMPONENTS LEVEL (E.G. STANDARD PRIOR ART, PC HARDWARE COMPONENTS, E.G. Y. 1993 US FEDERAL NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGIES (NIST'S) CLIPPER CHIP/CAPSTONE PROGRAM, E.G. NEWER POST-Y. 2004, CRYPTO-PC DESIGNS OF THE NON-PROFIT, TRUSTED COMPUTING GROUP (TCG (R)) (WWW.TRUSTEDCOMPUTINGGROUP.ORG) OF DECEMBER OF Y. 2003, E.G. EVEN

NEWEST IN ACTUAL MASS PRODUCTION IN Y. 2007, CRYPTO-DIGITAL SIGNAL PROCESSOR (CRYPTO-DSP), AND Y. 2007 CRYPTO-MICROPROCESSOR (C-uP, C-PC, C-HW) DESIGNS (WWW.TRUSTEDCOMPUTINGGROUP.COM (WWW.TRUSTEDCOMPUTINGGROUP.ORG)) AT THE HEART OF THE NEWEST, HIGH SECURITY, Y. 2007 DIGITAL CELLULAR NETWORKS, THE LOWER LEVEL PC SOFTWARE AT THE OPERATING SYSTEM (OS) COMPONENTS LEVEL, AND THE HIGHER LEVEL 'CRYPTO ARCHITECTURE LEVEL' OF THIS PRESENT APPLICATION. THE PRESENT APPLICANT IN ORDER TO DISTINGUISH HIS OWN SUBSEQUENTLY SHOWN, ORIGINAL SLIGHTLY OVERLY BROAD CLAIMED PATENT, OVER NARIN ET AL (DIFONZO IS ASSUMED AS POST-ART TO THE PRESENT APPLICANT'S PATENT AS DISCUSSED JUST BELOW), PROPOSES TO RESTRICT HIS OWN PATENT CLAIMS TO THE HIGHER LEVEL, CRYPTO-ARCHITECTURE LEVEL PATENT (TIEING TOGETHER 100% CRYPTO-HARDWARE SYSTEM COMPONENTS AND NON-CRITICAL PRIOR ART HARDWARE COMPONENTS, INTO A WORKABLE COMMERCIAL CRYPTOGRAPHY SYSTEM), WHILE ASSUMING THE EXISTANCE AT A LOWER COMPONENTS LEVEL, OF MINIMAL CRYPTO-DIGITAL SIGNAL PROCESSOR (C-DSP) CHIPS (WWW.TRUSTEDCOMPUTINGGROUP.ORG), AND CRYPTO-MICRO-PROCESSOR CHIPS (C-uP) (WWW.TRUSTEDCOMPUTINGGROUP.COM (WWW.TRUSTEDCOMPUTINGGROUP.ORG)), GIVING THE HIGHEST LEVELS OF COMMERICAL CRYPTO-SECURITY FOR CRYPTO-KEYS (E.G. SECRET KEYS, E.G. 1-TIME USE ONLY SECRET KEYS CALLED SESSION KEYS, E.G. GROUP USE SECRET KEYS CALLED FAMILY KEYS, E.G. FAMILY KEY PASS-THRU ENCRYPTION KEYS, E.G. RESTRICTED SHARED PRIVATE/PUBLIC KEYS USED FOR PUBLIC KEY FAMILY KEYS IN PASS-THRU ENCRYPTION, E.G. PRIVATE KEYS OF A {PRIVATE KEY.N, PUBLIC KEY.N} ALWAYS PAIRED SET, OFTEN USED PUBLIC KEYS ONLY FOR CUSTOMER CONVENIENCE, OR LACK OF NETWORKED ACCESS AS IN PUBLIC KEY CRYPTOGRAPHY PASS-THRU ENCRYPTION).

The patent examiner in his 1st Office Action (1OA Dated: 09/12/2007) brings up the DiFonzo patent, but, does not specifically cite it in a 35 USC Section 103 ("obviousness") USPTO objection. The present applicant assumes that this is because his own USPTO PPA and USPTO DDP submissions, pre-date the DiFonzo patent's own USPTO DDP first official dating, with no official USPTO mention of a DiFonzo USPTO DDP dating, or an official documented, DiFonzo 'date of first invention' (e.g. eye-witnessed invention log). This is a highly relevant post art, found by the patent examiner's diligent search, which was missed in the present applicant's own patent search as being post art. The DiFonzo patent, also importantly post-dates the present applicant's present invention.

CASE 2: J. DiFonzo (US Patent Pub. No.: US 205/0027991 A1, Publication Date: 02/03/2005, US Patent App. No.: 10/874,712, USPTO App. Filing Date: 06/23/2004, Provisional US Patent App. No. 60/480,821, PPA Filing Date: 06/23/2003),

DIFONZO PATENT BRIEF SUMMARY AND BRIEF AND HIGHLY RELEVANT PARTS LISTING: The present applicant states that the DiFonzo patent, was specifically designed to do wireless smart card 100, based secure or custom encrypted ("encrypted text"), digital media distribution over public global Internet/Web networks. The DiFonzo patent's higher level, crypto-architecture uses innovative new art, public key cryptography algorithms combined with much faster to execute, secret key cryptography algorithms (hybrid key cryptography), and also prior

art protocols, new art based upon wireless smart card 100, physical centralized, distribution from a central ITU X.509 defined Certificate Authority (ITU X.509 CA) (e.g. commercial music-movies CA, e.g. commercial banking CA, etc.), converted to a pre-programmed smart card distribution function, and also each X.509 Certificate Authority (CA), acting as a public key publication server over the global Internet/Web. Various per industry CA subordinate in DiFonzo crypto-architecture, digital media distribution vendors (e.g. a certain music vendor brand), have various subset knowledge of the crypto database information on a strict need to know bases. While DiFonzo also emphasizes 'new art/emerging art' authentication using assumed DiFonzo system standard, hardware of a very low cost (pennies per IC), wireless transceiver 210 ("RF ID smart card"), invented at MIT during the early 1990's using modified industry standard, very short-range (max. <= 10 [feet]) wireless "Bluetooth (IEEE Standard)" technology integrated with prior art, non-wireless smart card 100, technology. The DiFonzo patent also includes a commercial 'neutral trusted 3rd party' supplied kiosk 300 (e.g. airport lounger, e.g. coffee shop, e.g. restaurant) which has the global Internet/Web connection and can be used to on demand, download from Web server down to kiosk, 1-time use only secret key or session key, custom encrypted digital media for storing upon kiosk, public customer removable, various types of prior art, permanent digital media formats (e.g. CD (R), DVD (R), memory stick), kiosk dispensed from a media output slot 370, and only after e-payment using a kiosk's, bank card reader 320, while the not completely defined in the technical material, DiFonzo authentication device 200 (e.g. any low-cost commercial authentication device, e.g. wireless smart card reader, e.g.

any bio-ID reader), is present applicant assumed to first uniquely authenticate or uniquely identify to commercial security standards of probability, the customer, and also allow some means of wireless transfer of the custom 1-time use only secret key (session key), download to the wireless smart card for storage, the thus programmed wireless smartcard having to be in proximate Bluetooth, max. 10 foot range of any intended device used to 'play-back' the physical custom session key encrypted digital media using inserted into the wireless connected, DiFonzo player, prior art physical digital media (e.g. CD, DVD, EEPROM stick, EEPROM card, etc.).

DEFONZO PATENT PROBLEM 1: The DiFonzo patent application fails in expert crypto-analysis using the standard crypto-analysis methods mentioned in: REFERENCE 1: Bruce Schenier, Applied Cryptography 2nd Edition (standard software engineer's public key cryptography reference textbook), pp's 758], and, REFERENCE 2: Alfred DeMenzes et al, Applied Cryptography (standard Ivy League cryptography textbook), pp's 780], even for the low levels of low-cost and ease of use, commercial cryptography, being that DiFonzo is missing of key, pass-thru encryption algorithms, and is highly susceptible to standard cryptography based 'hacker attacks' of:

ATTACK 1: physical wiretapping of crypto keys by ace hardware engineering trained crackers [REF 1. B. Schenier, Applied Cryptography (the standard software engineer's public key cryptography reference text), 2nd Edition, p. 587], [REF 2, A.

DeMenzes et al, Applied Cryptography (standard Ivy League cryptography text), pp's 13], and

ATTACK 2: a well known, software hackers attack of simply digitally recording the unique encrypted keys, transmitted over a wireless bus or wired bus keys, and simply re-using them at will in custom encrypted form (recorded replay attack) [REF 1, (standard software engineer's public key cryptography reference textbook) Bruce Schenier, Applied Cryptography, 2nd edition, pp's 58 - 59], [REF 2, (standard Ivy League cryptography reference textbook) Alfred DeMenzes et al, Applied Cryptography, pp's 42, 417].

NOTE: The present applicant has done his own skilled crypto-analysis, being a skilled software engineer with a B.S. degree in Mathematics with a Computer Science option from California State University, Los Angeles, followed by a Masters in Computer Science degree from USC. The present applicant has also worked full-time, in the S. California, commercial and military aerospace industry for over 12 years, in addition most of the last decade the present inventor has spent in proprietary hi-tech and proprietary low-tech product development as President of his own new hi-technology, and/or low-technology, engineering design firm.

These 2 present inventor crypto-analyzed, alleged fatal flaws of the DiFonzo patent, can be easily repaired with standard cryptography methods of:

ATTACK 1 REMEDY: 'pass-thru encryption' [REF 1, (standard software engineer's public key cryptography textbook), B. Schenier, Applied Cryptography, 2nd edition, pp's 58 - 59], [REF 2, (standard Ivy League cryptography text), A. DeMenzes et al, Applied Cryptography, pp's 42, 417], and

ATTACK 2 REMEDY: use of either serial numbers (needing real-time serial number incrementing) or else, 'trusted computer' protected, strong cryptography levels, secure date-stamps and also strong cryptography levels, secure time-stamps [REF 1, (standard software engineer's public key cryptography textbook), B. Schenier, Applied Cryptography, 2nd Edition, pp's 58 - 59], [REF 2, (standard Ivy League cryptography text) A. DeMenzes et al, Applied Cryptography, pp's 42, 417].

DEFONZO PATENT PROBLEM 2: The DiFonzo patent application neglecting easy to fix ATTACK 1, fails in the not so easy to fix, most modern commercial crypto-hardware design trend (e.g. non-profit Trusted Computing Group (TCG) started by Mr. Alan Kaye, a leading East coast data processing marketing consultant worried about the major on-slaught upon commercial data processing security and consumer confidence losses, caused by the many hacker tools and tricks, in December of y. 2003 (www.trustedcomputinggroup.org)) as referenced in the non-profit, December of y. 2003 founded, Trusted Computing Group (www.trustedcomputinggroup.org). NOTE: An earlier y. 1999 Mr. Alan Kaye founded, highly related group, was called the non-profit, Trusted Computing Platform Group (R) (TCPG (R)), which basically folded up by

early y. 2003, due to technical design failure and 200 non-agreeing commercial vendors, in forcing a 100% 'bottom-up' 'trust granting model' at the PC hardware, Input/Output (I/O) peripheral plug-in card level, being that the original TCPG (R) architecture, was highly prone to expert hardware engineer wiretapping attacks, insecure standard commercial digital hardware, and over 200 in-fighting corporate vendor members not able to agree on a secure commercial solution. The original TCPG (R) of years 1999 - early 2003, also lacked a higher level crypto-architecture model (e.g. US DOD Conditional Access II smart card (US DOD CA II), vs. US DOD CA I based upon the commercial Sun (R) Java card standard) program's smart card, e.g. W. European Conditional Access For Europe (CAFE) developed a tiny palm-top, e-commerce terminal, also was related, Research of advanced broadband Communications for Europe (RACE), standards for smart cards and standard cryptography protocols [REF 1, B. Schneier, 2nd Edition, pp's 605 - 607], e.g. Mid-1990's technology, highly crypto-analytically insecure, Apple (R) licensed, Fairplay (R) cryptography architecture for the I-Tunes (R) store (allegedly based upon the algorithms of the USPTO, S. Ansell et al, patent No. 6,367,019, Issue Date: 4/2/2002 [REF 10, Ansell et al]) for workable commercial key distribution (e.g. provided by the present applicant's patent). DiFonzo even with an assumed low-cost and 'ease of use' requirements of commercial level strong cryptography, is restricted to late 1990's hardware components level technology, since, DiFonzo does not use a standard assumed, crypto-digital signal processor (C-DSP) component (present applicant's part number 880) or else a very similar crypto-micro-processor (C-uP) component, a standard micro-processor based around a hardware embedded

crypto-micro-controller with 'crypto-core' hardware features (present applicant's 'provided by' claims 1, with a present applicant proposed move into the new technical material section while removing the overt claims legal language).

The patent examiner does not cite any 35 USC Section 103 ("Obviousness") 'prior art' objections to the present applicant's invention in view of DiFonzo. The present applicant having access to only 'USPTO file wrapper' summary dates for DiFonzo and his own patent application's USPTO 'file wrapper' dates, assumes that this patent examiner's lack of citing DiFonzo as prior art, is due to DiFonzo's technical material as post-dating the present applicant's entire 'USPTO file wrapper' patent material.

The present applicant's present patent application has been widely published world-wide, since, USPTO publication No.: US 2005/0195975 A1, since USPTO Publication Date: Sep. 8, 2005, quickly becoming for the last several years, the number 1, 'popularity ranked,' Google (R) brand of keyword based search entry, for the combined Google (R) brand of global Internet Web search engine, keyword entries of: 'digital media distribution' and 'smart cards.' Also all parties of relevance, especially the present applicant, are relying upon the USPTO's very professinal, and very strict archiving and documentation standards for proper patent material dating, as well as being the principal US Federal government agency, protecting the original inventor's future patent rights.

The present applicant's patent application material has already as of y. 2007, been used as a key shaper of future technology, as per USPTO's highly efficient and highly respectful of US Federal law, legal process of safe-guarding original inventor's patent rights, intended by 35 USC Section 101 - 103, patent law specifications [US Constitution's main body Article I (legislative powers) Section 8], USPTO currently defined through US Federal law mandated, USPTO's new technology development model for US Patent application qualified products, of keeping trade secret information confidential until full USPTO patent filing, after which, the USPTO legally allows highly necessary, full invention public publication disclosure, and badly needed open, non-copyrighted, patent application publication, facilitating early public discussion of key technical material, necessary for rapid and legal, commercialization of relevant US Patent application applied for commercial products.

Conclusion to REMARKS section.

The present applicant believes that his current Amendment A in direct response to the patent examiner's 1st Office Action letter dated: 09/12/2007, addresses all present patent examiner objections, and brings the Amendment A patent application up to current 35 USC Sections 101 - 103, US Federal law standards [US Constitution, Article I Section 8], and also detailed procedural law implementation in the current USPTO MPEP standards.

Very Respectfully Yours,

Signature

EL 689138392 US

USPS Xpress Mail No.

KEVIN KAWAKITA

Inventor

GLENDALE, CA

USPS Postal Office Location

5812 Temple City Bl. #100

Temple City, CA 91780

Mailing Address

kevinkawa777@msn.com

kevinkawa777@msn.com

Contact Info.